Short Papers

Markov Decision Processes for Fake Accounts Detection

Alexander Semenov(✉), Gaurav Pandey, and Denis Kotkov

Faculty of Information Technology, University of Jyvaskyla, Jyväskylä, Finland
{alexander.v.semenov,gaurav.g.pandey}@jyu.fi, kotkov.denis.ig@gmail.com

Abstract. Detection of fake accounts on the Internet is usually considered as a one-time classification problem. However, with each subsequent action of the user, the chances of him to be considered as fake would change. Therefore, it is intuitive to see fake account detection as a sequential decision problem. Markov Decision Process (MDP) is an effective method for sequential decision making. In this paper, we define fake account detection as a sequential decision making problem and describe a MDP based definition for it.

Keywords: Fake account detection · Markov decision process
Machine learning

Extended Abstract

The use of fake identities presents a serious challenge for trustworthy information exchange on the Internet. Fake identity use refers to the use of such an identifier by a person to whom the identifier does not point to. This can be the result of identity theft or the creation of a fake identifier that does not point to any real person. State of the art methods of fake account detection typically involve application of supervised machine learning (where identities are classified as fake or benign), or anomaly detection algorithms; input data for these algorithms is particular set of features, depending on the application domain (such as texts posted by the user, his profile data, ego-network, etc).

Majority of current research presents fake account detection as one-time classification; however it is more natural to represent it as a sequential decision problem, where decision-maker performs certain actions that lead to identification of the fake account. This is because, with each action of a user (e.g. tweet content, frequency change of tweeting, addition of friends, etc.), the chances of him being a fake account can change. Therefore, we suggest to view fake account detection as a sequential decision problem, where actions of a *system* depend on the observed state of the identifier. Markov Decision Process (MDP) can be employed to model the problem, as it is a prominent model for sequential decision making. Article [3] applies Markov Reward process for sequential anomaly detection; reinforcement learning is applied to learn optimal customer interactions in [1].

X. Chen et al. (Eds.): CSoNet 2018, LNCS 11280, pp. 539–540, 2018.
https://doi.org/10.1007/978-3-030-04648-4

A Markov decision process is a 5-tuple $(S, A, P_a(S_i, S_j), R_a(S_i), \gamma)$, where S is a set of states, A is a set of actions, $P_a(S_i, S_j)$ is the probability that action a in state S_i will lead to S_j, $R_a(S_i)$ is the reward on taking action a on state S_i, γ is the discount factor [2]. The goal of decision maker is to find a *policy* $\pi(a|S_i)$ that defines behavior of the decision maker such that total cumulative reward will be maximized. We define following discrete time MDP notations for fake account detection:

Actions: Set of actions available to the decision maker that are aimed at helping to classify, or block the user. Examples of the actions are as follows: "Provide CAPTCHA test to use","Analyze CAPTCHA test response", "Block the user","Lock account for several minutes", "Unblock the user".

Observations: Actions of the user: send a message, like a post, repost a message, respond (or not) to CAPTCHA test

Rewards: Each action of the decision maker is associated with reward. Generally, reward is positive, when the user cannot pass the test, i.e. the bot was detected. Reward is negative when the user passes the test, since we cause inconvenience to a genuine user. Further, some actions (such as e.g. checking of the user by a human moderator) are considered expensive and incur negative reward. The best case is correct classification of all fake accounts.

History: sequence of interactions with a user: $\{o_1, a_1, ..., o_t, a_t\}$, where o_i represents and observation, and a_i represents an action. Examples: The user becomes active after locking period, The user changes his posting frequency, user abandons the account, etc.

States: We represent state of a single user as a full history of her interaction with the system. We assume the states as histories of all the users [1].

Transition Function: Transition function $P_a(S_i, S_j)$ is deterministically determined by the action and the change of states.

Objective: A policy $\pi(a|S_i)$ is the strategy that can be applied to any identity, based on all existing histories. The objective is to find an optimal policy π^*, maximizing cumulative reward, i.e. correct classification of all accounts with minimal false positives and "expensive" actions such as manual intrusion. In other words, we perform classification of a user based on histories of all users.

We defined MDP for fake account detection. Further, we will present algorithms for finding optimal policy, and compare it with supervised machine learning used for fake account classification. The learning process of the user in response to the actions taken by the system are not modeled in MDP. In future, we plan to look into stochastic games as a solution for fake account detection.

References

1. Silver, D., Newnham, L., Barker, D., Weller, S., McFall, J.: Concurrent reinforcement learning from customer interactions. pp. III-924-III-932. ICML (2013)
2. Szepesvári, C.: Algorithms for reinforcement learning. Synth. Lect. Artif. Intell. Mach. Learn. **4**(1), 1–103 (2010)
3. Xu, X.: Sequential anomaly detection based on temporal-difference learning: principles, models and case studies. Appl. Soft Comput. **10**(3), 859–867 (2010)

The Network of Causal Relationships in the U.S. Stock Market

Oleg Shirokikh[1], Grigory Pastukhov[2], Alexander Semenov[3], Sergiy Butenko[4], Alexander Veremyev[5], Eduardo Pasiliao[6], and Vladimir Boginski[5(✉)]

[1] Frontline Solver, Reno, NV, USA
olegshirokikh@gmail.com
[2] CSX Transportation, Jacksonville, FL, USA
grigoriypas@gmail.com
[3] University of Jyväskylä, Jyväskylä, Finland
alexander.v.semenov@jyu.fi
[4] Texas A&M University, College Station, TX, USA
butenko@tamu.edu
[5] University of Central Florida, Orlando, FL, USA
{Alexander.Veremyev,Vladimir.Boginski}@ucf.edu
[6] Air Force Research Laboratory, Eglin AFB, Valparaíso, FL, USA
eduardo.pasiliao@us.af.mil

Abstract. We propose a network-based framework to study causal relationships in financial markets and demonstrate the proposed approach by applying it to the entire U.S. stock market. Directed networks (referred to as causal market graphs) are constructed based on stock return time series data during 2001–2017 using Granger causality as a measure of pairwise causal relationships between all stocks. We consider the dynamics of structural properties of the constructed network snapshots, group stocks into network-based clusters, as well as identify the most "influential" stocks via a PageRank algorithm. The proposed approaches offer a new angle for analyzing global characteristics and trends of the stock market using network-based techniques.

Keywords: Stock market · Big data · Network analysis
Causal market graph · Granger causality

Extended Abstract

The modern stock market is a complex interconnected system, where various "local" factors can cause "global" changes in the behavior of the entire market. For instance, favorable or unfavorable economic conditions in certain countries, or in certain market segments, may affect other countries and industries and potentially cause positive or negative fluctuations that span the entire U.S. and international markets. The idea of describing causal relationships between different components of the market system has been addressed in several recent

X. Chen et al. (Eds.): CSoNet 2018, LNCS 11280, pp. 541–542, 2018.
https://doi.org/10.1007/978-3-030-04648-4

studies. The survey by [3] discussed the concept of *contagion* in financial markets, which essentially implies the propagation of impact (such as risk) between different components of the market. Clearly, a *network-based* model is a natural way to mathematically represent these "contagion" processes; however, the principles for constructing the networks that reflect certain types of processes may vary depending on the purpose of the study.

Possibly the most intuitive technique for constructing a network-based (or, graphical) model of the market is to represent its elements (e.g., stocks) as nodes and connect the nodes by links (arcs) based on pairwise correlations between the corresponding entities (i.e., the correlations between stock price fluctuations over a certain period of time). Such an approach was studied by [1, 2] in the context of identifying large correlated clusters and diversified portfolios in the U.S. stock market. Although the pairwise correlation measure has its merit in certain situations, its substantial drawback is in inability to produce *directed* links between entities, that is, establish the direction of "contagion" (i.e., the propagation from node i to node j vs. the propagation from node j to node i).

In this work, we construct and analyze a *directed* network model, which rigorously describes *causal relationships* between all pairs of stocks in the U.S. stock market using the concept of *Granger causality.* The motivation behind this approach was investigating the possibility of drawing meaningful conclusions about the behavior and trends of the entire market *solely* based on a rigorously defined quantitative causality measure, as an alternative to studying these causal relationships based on subjective criteria, such as analysts' opinions, etc., which may not be easily quantifiable. It should be noted that Granger causality, which will be formally defined later in this paper, can be used to determine whether the time series describing stock i is useful in predicting the behavior of stock j, which should not be confused with the statement "the increase/decrease in the price of stock i causes the increase/decrease in the price of stock j". Granger causality appears to capture certain structural properties of the stock market that reflect global tendencies in its behavior. In particular, we investigate various aspects of connectivity patterns and the dynamics of structural properties of the constructed network snapshots. Moreover, the proposed network representation is used to group stocks into network-based clusters and identify the most "influential" market entities (sectors, industries and individual stocks).

Acknowledgments. Work of A. Semenov was funded in part by the AFRL European Office of Aerospace Research and Development (grant no. FA9550-17-1-0030)

References

1. Boginski, V., Butenko, S., Pardalos, P.M.: Statistical analysis of financial networks. Comput. Stat. Data Anal. **48**, 431–443 (2005)
2. Boginski, V., Butenko, S., Pardalos, P.: Mining market data: a network approach. Comput. Oper. Res. **33**, 3171–3184 (2006)
3. Sowers, R., Giesecke, K.: Contagion. SIAM News p. 18 October 2011

Author Index